Amendments to the Specification

The following refers to the paragraph numbering used in the application as published.

Please replace paragraph [0001] with the following replacement paragraph:

[0001] The present invention relates to [[a]] the field of cryptography, in particular to the issuance of certificates to mobile clients in a ~~(Public Key Infrastructure)~~ Public Key Infrastructure (PKI).

Please replace paragraph [0006] with the following replacement paragraph:

[0006] In order to permit one correspondent to communicate securely with another it is necessary that each is confident of the authenticity of the other and that the public key used by [[are]] each of the correspondents to verify signatures or decrypt messages is in fact the public key of the other correspondent. This is typically achieved through the use of a certificate issued by a party trusted by both correspondents. The initiating correspondent requests the trusted party to sign the public key with the trusted parties own private key and thereby create a certificate.

Please replace paragraph [0020] with the following replacement paragraph:

[0020] The infrastructure organized under the CA is known as a public key infrastructure (PKI) and commonly defined as a set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, revoke and destroy certificates and keys based on public key cryptography, in a distributed computing system. A PKI may include a certificate issuing and management system (CIMS) ~~whereby~~ which includes the components of the PKI that are responsible for the issuance, revocation and overall management of the certificates and certificate status information. A CIMS includes a CA and may include Registration Authorities (RAs), and other subcomponents.

Please replace paragraph [0021] with the following replacement paragraph:

[0021] The advent of new technologies, such as 2.5G and 3G networks, which provide enough bandwidth to support audio and video content, and seamless global roaming for voice and data has given rise to a new class of mobile devices such as network-connected personal digital assistants (PDAs) and ~~WAP-enabled~~ Wireless Application Protocol (WAP) enabled mobile phones generally referred to as constrained devices. This trend effectively extends traditional personal computer application services to mobile devices, such that traditional e-commerce is performed on mobile devices, that is, mobile commerce. As in e-commerce there is still a need for the client to provide identification, authentication and authorization to the merchant, authentication being the act of verifying the claimed identity of the station or originator, while ~~authentication~~ authorization involves the use of certificates via a certification authority.

Please replace paragraph [0024] with the following replacement paragraph:

[0024] Accordingly, it is an object of the present invention to obviate or mitigate at least one of the above disadvantages.

Please replace paragraph [0035] with the following replacement paragraph:

[0035] Secure communications between the correspondents 12 and 14 may be implemented by providing a public key infrastructure (PKI) 18 to the network 16. The PKI 18 includes a registration authority (RA) 19 to receive and process requests for a certificate from correspondent 12 and one or more certification authorities (CA) 20. The PKI 18 provides a standards-based certificate issuance and management system (CIMS) platform for issuing, publishing and revoking public key certificates. Each of the correspondents 12, 14 have the public key of the [[(CA)]] CA 20 embedded in the devices so as to be able to verify messages sent by the [[(CA)]] CA 20 and signed with the corresponding private key [[or]] of the [[(CA)]] CA 20.

Please replace paragraph [0044] with the following replacement paragraph:

[0044] Upon receiving the data package, the correspondent 14 constructs the address of the certificate based on the information provided in the certificate locator 24, uses that address to retrieve the certificate from the ~~LDAP directory, 22,~~ Lightweight Directory Access Protocol (LDAP) directory 22, extracts the public key of the correspondent 12, and verifies the CA's signature in the certificate using the embedded public key of the CA 20. The message from the correspondent 12 is then verified using the extracted public key and the secure transaction completed.

Please replace paragraph [0046] with the following replacement paragraph:

[0046] The procedure for obtaining a certificate from the registration authority 19 for the correspondent 12 is shown on the diagram of FIG. 2. Initially, the correspondent 12 establishes a trusted relationship with the registration authority 19. A secure connection is established between the client 12 and RA 19 in accordance with one of the established protocols, such as ~~WLTS, SSL or TLS.~~ Wireless Layer Transaction Security (WLTS), Secure Sockets Layer (SSL), or Transport Layer Security (TLS). After the secure connection is established, a certificate request 23 is prepared as indicated at 40. The certificate request 23 includes a set of information that will vary from application to application. In one example indicated schematically at FIG. 3 however the certificate request 23 includes a header 24 to indicate that the message is a certificate request, the correspondents public key 25, identifying information [[26]] 28 associated with the initiating correspondent 12, such as a social insurance number or ~~mothers~~ mother's maiden name, and a time varying indicator 27 such as a date and time stamp or counter.